UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,782	03/03/2000	Kouya Tochikubo	04329.22444	7469

22852 7590 11/21/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 11/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/518,782	Applicant(s) TOCHIKUBO ET AL.	
	Examiner Mossadeq Zia	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 03/03/2000 .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: on page 4, line 18, the phrase "defined in claim 3" should be omitted or re-state "as mentioned above", or the like, since it is trying to point to the cryptographic communication terminal that was discussed earlier in the specification. If this is not the objective, then the applicant needs to define the terminal in the specification, and not reference the definition in the claim.

Claim Objections

1. Claim 14 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent may depend on claims in the alternative only (claim 1 or 7). See MPEP § 608.01(n). Accordingly, claim 14 has not been further treated on the merits.

2. Claim 10 is objected to because of the following informalities: the phrase "said cryptographic communication terminal defined in claim 3" can just be stated as "said cryptographic communication terminal" because this was stated in claim 9 on which this claim is dependent upon. Therefore it is understood that it is the same cryptographic communication terminal being referenced.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claims 1, 7, 13, 15 are rejected under 35 U.S.C. 102(b) as anticipated by Patent No. 5,199,069, Barrett et al.**

5. Regarding claim 1, Barrett discloses a cryptographic communication terminal comprising:

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication (col. 3,line 58-60), and outputting a designated cryptographic algorithm (synchronization, col. 4, line 14-16, 29-31);

a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key (select a different key, col. 5, line 68, col. 6, line 1-5, 8);

control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication (col. 2, line 15-17; col. 3, line 54-56); and

encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted (col. 4, line 60-62; col. 5, line 21-23).

6. Regarding claim 7, Barrett disclose claim 1 above and further discloses said

control means instructs (controller, col. 3, line 26-27) said cryptographic algorithm storage section to output a requested cryptographic algorithm (control signal, col. 4, line 5-6)

upon receiving a transmission request (binary signal, col. 3, line 68, col. 4, 1) for any one of the cryptographic algorithms stored in said cryptographic algorithm storage section, and

said encryption/decryption means encrypts the requested cryptographic algorithm as the information to be transmitted (col. 4 , line 29-31, col. 7, line 66-68, col. 8, line 1-2).

7. Regarding claim 13, Barrett disclose claim 1 above and further shows a communication system comprising not less than two cryptographic communication terminals (col. 1, line 60-62).

8. Regarding claim 15, see reasoning for claim 1.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 2, 3, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069 Barrett et al. in view of Patent Application Publication US 2000/0046564, Masuda et al.**

11. Regarding claim 2, Barrett discloses a terminal according to claim 1, and shows that cryptographic algorithm storage section stores an cryptographic algorithm (encryption circuits, Barrett, col. 3,line 57-60), but fails to show said terminal further comprises cryptographic algorithm decryption means for decrypting the encrypted cryptographic algorithm.

Masuda shows a system where a medium for storing (algorithm storage section) an algorithm encrypted together with the data. A loader in the device driver 22 loads the encrypted algorithm 34 into the PC (terminal) 11, transmits it to the server 33 (decrypting means), and requested the server 33 to decrypt the algorithm 34. Then the loader 31 receives the algorithm decrypted by the server 33 and transmits it to the decrypting unit 23. The decrypting unit 23 decrypts the data according to transmitted algorithm (Masuda, fig. 6, pp. 2, para. 0046).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Masuda to include encrypted decryption algorithm such that Barrett gains the advantage of further improving the security for the data stored on the storage medium (Masuda, pp. 1, para. 0017).

12. Regarding claim 3, Barrett and Masuda discloses claim 2 above, and further discloses said key information storage section stores a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm (Masuda, pp. 1, para. 0016) as well as the key for cryptographic communication (Barrett, col. 4, line 1-3).

13. Regarding claim 16, see reasoning for claim 2.

14. **Claims 4, 5, 9, 11, 12, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barrett et al. and Masuda et al. in further view of Patent No. 5,491,749, Rogaway.**

15. Regarding claim 4, Barrett discloses claim 3 above, but fails to clearly disclose the key for the encrypted algorithm is a key for secret key cryptography.

However, Rogaway teaches Diffie-Hellman key exchange where the purpose of the technique is to publicly exchange information that can be combined to generate a shared secret key (secret key), which can be utilized for particular communication sessions (Rogaway, fig. 2,

col. 6, line 5-7). Furthermore, Rogaway teaches Bellovin and Merritt encrypted key exchange, which is an elaboration of the Diffie-Hellman key exchange (Rogaway, fig. 3, col. 6, line 36-37). This technique can be utilized to periodically generate short-live session keys (col. 6, line 65-66).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Rogaway to include key exchange to gain the advantage of protecting communication channels which may be subjected to passive and active adversaries (Rogaway, col. 6, line 25-28).

16. Regarding claim 5, Barrett discloses claim 3 above, but fails to clearly disclose the key for the encrypted algorithm is a key for public key cryptography.

However, Rogaway teaches Diffie-Hellman key exchange where the purpose of the technique is to publicly exchange information (public key) that can be combined to generate a shared secret key, which can be utilized for particular communication sessions (Rogaway, fig. 2, col. 6, line 5-7). Furthermore, Rogaway teaches Bellovin and Merritt encrypted key exchange, which is an elaboration of the Diffie-Hellman key exchange (Rogaway, fig. 3, col. 6, line 36-37). This technique can be utilized to periodically generate short-live session keys (col. 6, line 65-66).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Rogaway to include key exchange to gain the advantage of protecting communication channels which may be subjected to passive and active adversaries (Rogaway, col. 6, line 25-28).

17. Regarding claim 9, Barrett discloses claim 3 above, but fails to show when the algorithm decryption key is requested from the partner, said apparatus inputs the corresponding algorithm

decryption key as the information to be transmitted to the partner to said encryption/decryption means.

However, Rogaway teaches Diffie-Hellman key exchange where the purpose of the technique is to publicly exchange information that can be combined to generate a shared secret key (decryption key), which can be utilized for particular communication sessions (Rogaway, fig. 2, col. 6, line 5-7). Furthermore, Rogaway teaches Bellovin and Merritt encrypted key exchange, which is an elaboration of the Diffie-Hellman key exchange (Rogaway, fig. 3, col. 6, line 36-37). This technique can be utilized to periodically generate short-live session keys (col. 6, line 65-66).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement Barrett as per teaching of Rogaway to include key exchange technique to gain the advantage of protecting communication channels which may be subject to passive adversaries (Rogaway, col. 6, line 25-27).

18. Regarding claim 11, Barrett and Rogaway teach claim 9 above, and further teach key encrypt means for, when the key for the encrypted algorithm is requested from said cryptographic communication terminal, encrypting the key (shared secret, Rogaway, col. 6, line 50-55) for the encrypted algorithm (signals, Barrett, col. 3, line 66) to be transmitted, and inputting the encrypted key for the encrypted algorithm, as the information to be transmitted, to said encryption/decryption means (Rogaway, col. 5, line col. 4, line 1-2, col 5, line 22).

19. Regarding claim 12, Barrett and Rogaway teach claim 11 above, and further teach that key encryption means encrypts the key for the encrypted algorithm by using a key unique

(authentication key) to a cryptographic communication terminal of the partner (Rogaway, col. 6, line 50-52).

20. Regarding claim 18, see reasoning for claim 11.

21. **Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069 Barrett et al. in view of Patent No. 5,721,777, Blaze.**

22. Regarding claim 6, Barrett discloses claim 1 above, but fails to clearly disclose said key information storage section stores an encrypted key, and said terminal further comprises key information decryption means for decrypting the encrypted key.

However, Blaze teaches a cryptographic key management system for a cryptographic module with a (Blaze, fig. 1, element 23 and fig. 2) secure storage areas comprising of working memory 201, key storage area 202 (Blaze, col. 4, line 36-37), where the key storage area 202 contains encrypted escrow key and the encrypted audit key (Blaze, col. 4, line 43, 45, 55-56). For an escrow agent to use the smart card (which contains key storage area; Blaze, fig. 1, element 20, 23), the escrow key passphrase (decryption of key) must be revealed to the escrow agent.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Blaze to include a key management system to gain the advantage of accessing critical data files (stored encrypted keys) when the only person who know the keys to those files are unavailable (Blaze, col. 1, line 29-30).

23. **Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069 Barrett et al. in view of Patent No. 4,484,025, Ostermann et al.**

24. Regarding claim 8, Barrett discloses claim 1 above, and further discloses a partner with which said terminal communicates is an apparatus including said cryptographic communication terminal (Barrett, col. 2, line 32-34), but fails to show said terminal requests the partner for a new cryptographic algorithm and/or a key for a corresponding encrypted algorithm, decrypts a corresponding response by using said encryption/decryption means, stores the requested cryptographic algorithm in said cryptographic algorithm storage section upon receiving the cryptographic algorithm, and stores the requested key for the encrypt algorithm in said key information storage section upon receiving the key.

However, Ostermann teaches a system for enciphering and deciphering data (Ostermann, fig. 1) where the system cipher algorithm is transmitted from the cipher program storage 18 over a data transmission channel 20 to the program memory 22 of the programmable cipher computer (Ostermann, col. 2, line 38-41). It further shows that the transmission of a cipher program can also be initiated at the programmable cipher computer 12 by means of a cipher request initiator 29. This permits the transmitting terminal 1 to request that the cipher algorithm be transmitted from the receiving terminal 2 prior to transmission (Ostermann, col. 3, line 4-9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Ostermann such that exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

25. Regarding claim 20, see reasoning for claim 8.

26. **Claims 10, 17, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069 Barrett et al. in view of Patent No. 5,491,749, Rogaway in further view of Patent No. 4,484,025, Ostermann et al.**

27. Regarding claim 10, Barret and Ragaway discloses claim 9 above, and but fails to discloses an update cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms decrypted by using a key for the encrypted algorithm, and said control means, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructs said update cryptographic algorithm storage section, in place of said cryptographic algorithm storage section, to output the requested cryptographic algorithm as the information to be transmitted.

However Ostermann teaches that cipher algorithm (fig. 1) is transmitted from the cipher program storage (element 18) over a data transmission channel (element 20) to the program memory (Ostermann, col. 2, line 38-41). The data transmitted between the first and the second terminals is enciphered in accordance with the cipher program code and the cipher key stored in the programmable computer (Ostermannm col. 1, line 64-68). Furthermore, it shows that the storage computer is provided with a long-term memory for storage of a plurality of different cipher programs (Ostermann, col. 2, line 59-60).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barret and Ragaway as per teaching of Ostermann such that exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

28. Regarding claim 17, 19, and 21, see reasoning for claim 10.

Conclusion

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100